

PCT/ZA 2004/00012

# Sertifikaat

REPUBLIEK VAN SUID AFRIKA

PATENT KANTOOR  
DEPARTEMENT VAN HANDEL  
EN NYWERHEID



# Certificate

REPUBLIC OF SOUTH AFRICA

PATENT OFFICE  
DEPARTMENT OF TRADE AND  
INDUSTRY

Hiermee word gesertifiseer dat  
This is to certify that

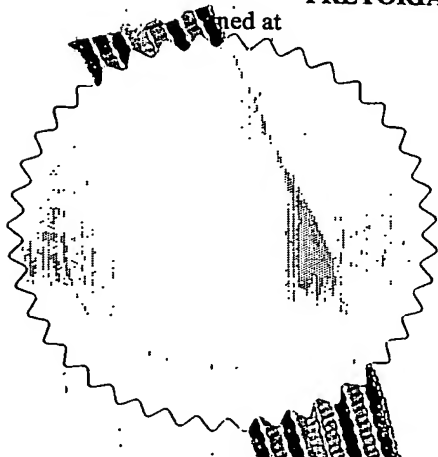
the documents annexed hereto are true copies of:

Application forms P.1, P2 and provisional specification and drawing  
of South African Patent Application No. 2003/8654 as originally filed  
in the Republic of South Africa on 6 November 2003 in the name of  
RADIO SURVEILLANCE TECHNOLOGIES (PTY) LTD and an applicant  
substituted to SELVANATHAN NARAINSAMY on 15 June 2004 for an  
invention entitled: " CREDIT CARD TRANSACTION VERIFICATION  
SYSTEM ".

Geteken te  
signed at  
PRETORIA

in die Republiek van Suid-Afrika, hierdie  
in the Republic of South Africa, this

dag van  
day of  
2 December 2004



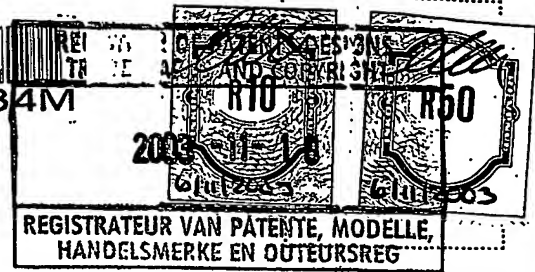
Registrar of Patents

REPUBLIC OF SOUTH AFRICA		REGISTER OF PATENTS		PATENTS ACT, 1978	
Official number		Lodging date - provisional		Acceptance date	
21 04 2003 / 86.54		22 6 November 2003			
International classification		Lodging date - complete		Grant date	
51		23		47	
Full name(s) of applicant(s)/patentee(s)					
71 Radio Surveillance Technologies (Pty) Ltd					
Applicant(s) substituted				Date registered	
71 SELWANATHAN NARAINSAMY				15.6.04	
Assignment - Assignee(s)				Date registered	
71					
Full name(s) of inventor(s)					
71 Andrew Gary Wright; Selvan Narainsamy					
Priority claimed		country		number	
		33		31	
		33		31	
		33		31	
Title of the invention					
54 Credit Card Transaction Verification System					
Addresses of applicant(s)/patentee(s)					
Suite 903, Tower B, Salisbury Centre, 349 - 351 West Street, Durban, South Africa					
74 Address for service					
PFT Burger reference: PP.3809.RAD					
PFT Burger, Patent & Trade Mark Attorneys					
10 Mount Argus Road, Umgeni Heights, Durban - PO Box 546, Durban 4000					
DOCEX 305 DURBAN					
TEL - 573 1054 FAX - 573 1058					
Patent of addition - no.				Date of any change	
61					
Fresh application based on:				Date of any change	

REPUBLIC OF SOUTH AFRICA  
PATENTS ACT, 1978  
Application for a patent and acknowledgement of receipt  
[section 30(1) - regulation 22]

FORM P1

CIPRO005784M



Official number		
21	01	2003/8654

PFT Burger reference
PP.3809.RAD

71	Full name(s) of applicant(s)	Radio Surveillance Technologies (Pty) Ltd
	Address(es) of applicant(s)	Selvanathan Narain Sany 15-6-04 Suite 903, Law Centre, 349 - 351 West Street, Durban, South Africa

54	Title of the invention
Credit Card Transaction Verification System	

<input checked="" type="checkbox"/>	The applicant claims the priority set out on the enclosed Form P2
-------------------------------------	---

21	01	This application is for a patent of addition to Patent Application no.
----	----	--

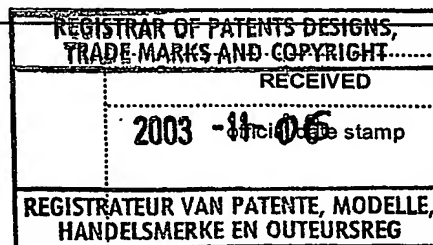
21	01	This application is a fresh application in terms of s37 and is based on Patent Application no.
----	----	--

This application is accompanied by:

- ☐ 1 A single copy of a provisional specification of 10 pages
- ☐ 2 Drawings of 1 sheet

74	Address for service
PFT Burger, Patent & Trade Mark Attorneys 10 Mount Argus Road, Umgeni Heights, Durban - PO Box 546, Durban 4000 DOCEX 305 DURBAN TEL - 573 1054 FAX - 573 1058	

Dated: 6 November 2003



PFT Burger, Patent & Trade Mark Attorneys

Registrar of Patents

REPUBLIC OF SOUTH AFRICA  
PATENTS ACT, 1978  
Provisional specification  
[section 30(1) - regulation 27]

FORM P6

Official number		
21	01	2003 / 8651

Lodging date	
22	6 November 2003

Full name(s) of applicant(s)	
71	Radio Surveillance Technologies (Pty) Ltd

Full name(s) of inventor(s)	
72	Andrew Gary Wright; Selvan Narainsamy

Title of the invention	
54	Credit Card Transaction Verification System

## Background to the invention

This invention relates to apparatus for and a method of processing financial transactions.

In this specification the terms "telecommunication" and "telecommunications" are used largely in the conventional sense of referring to communications on a telephone network, but the terms are not necessarily intended to be limited to such an interpretation in every instance. Where a wider interpretation is possible in the context, then the terms should be interpreted widely, such as to include two-way radio communications for instance.

## Summary of the invention

According to this invention, a financial transaction verification system comprises:

- a transaction processing client under control of either or both a merchant and a transaction initiator;

- a transaction processing server under the control of a financial services provider;

- a telecommunications server under control of either or both the financial services provider and a telecommunications service provider; and

- a programmable telecommunications client under the control of the transaction initiator;

the transaction processing client, the transaction processing server, the telecommunications server and the telecommunications client all being connected to or adapted for connection to at least one telecommunications network;

the transaction processing client being adapted to accept and record:

- data pertaining to a transaction initiated, in use, by the transaction initiator;

- and

- data pertaining to a financial account of the transaction initiator with the financial services provider; and

- to transmit the recorded data to the transaction processing server by way of the telecommunications network;

the transaction processing server being adapted, to make use of communications data pertaining to the transaction initiator previously stored with the financial services provider and to transmit a transaction authorisation request to the telecommunications server;

the telecommunications server being adapted to receive and transmit the authorisation request to the telecommunications client;

the telecommunications client being programmed:

- to require the entry of an authorisation code previously provided by either or both the financial services provider and the transaction initiator;

- if the incorrect code is entered, to transmit a transaction cancellation signal to either or both the transaction processing server and the transaction processing client; and

- if the correct code is entered to transmit a transaction authorisation signal to either or both the transaction processing server and the transaction processing client.

The transaction authorisation signal may be communicated directly to the transaction processing server or the telecommunications client or it may be routed to the transaction processing server indirectly by way of the telecommunications server.

The financial services provider may be a financial institution such as a bank.

The transaction initiator will then be the holder of an account with the financial institution and the transaction initiated in the system described above will, typically, be the purchase of goods or services or the transfer of funds to or from the account administered by the financial services provider for and in the name of the transaction initiator.

The financial transaction may be initiated in any one of a number of ways, including by way of a computer serving as an internet terminal or by way of a merchant point of sale (POS) terminal that accepts payment, in the form of credit card or cheque payments.

The telecommunications client is preferably a mobile telephone personal to the transaction initiator. This will allow better separation of the transaction authorisation component of the above mentioned process from the transaction initiation component of the process. This is because the initiation component will typically take place on a fixed line network to which the transaction processing client and the transaction processing server are connected, while the mobile telephone communicates on a mobile telephone network.

The invention includes a method of verifying a financial transaction comprising the steps of:

- initiating a transaction at a transaction processing client under control of either or both a merchant and a transaction initiator;
- accepting, transmitting and recording data pertaining to the transaction from the transaction processing client to the transaction processing server by way of a telecommunications network, together with data pertaining to a financial account of the transaction initiator with the financial services provider;
- supplying communications data pertaining to the transaction initiator previously stored with the financial services provider to the transaction processing server;
- transmitting an authorisation request pertaining to the initiated transaction to a telecommunications server which is under control of either or both the financial services provider and telecommunications service provider;
- transmitting the transaction authorisation request from the telecommunications server

to telecommunications client which is under the control of the transaction initiator, the telecommunications client being programmed to require the entry of a code previously provided by either or both the tsp and the transaction initiator; canceling the transaction if the incorrect code is entered; and If the correct code is entered transmitting a transaction authorisation signal to either or both the transaction processing server and the telecommunications client.

### **Brief description of the drawing**

The invention will be further described with reference to the accompanying drawing which is a flow chart illustrating one implementation of the invention.

### **Description of embodiments of the invention**

The financial transaction verification system of the invention is possibly best understood with reference to an example, one of which is illustrated in the flow chart referred to above.

The flow chart illustrates the example of a relatively simple financial transaction involving a point of sale (POS) payment terminal at which credit cards or cheques are used to pay for the purchase of goods. Using the example of a credit card, the credit card belongs to the person who makes a purchase and who will be referred to as the transaction initiator in this specification. The transaction initiator will have a credit card account linked to the credit card with a bank or other financial institution, which is referred to in this specification as a financial services provider.

The financial services provider operates and serves a network of point of sale terminals and other electronic transaction terminals, such as automated teller machines (ATM's) and the computers of its banking clients in circumstance where those computers serve as internet banking terminals.

This network of terminals is normally operated from a central servers or servers which, in this specification, are referred to as the transaction processing server.

In a typical credit card transaction, the transaction details are entered at the POS terminal (the transaction processing client) where the credit card is swiped to obtain details pertaining to the transaction initiator, typically the credit card account number held with the financial services provider.

The transaction processing client then dials up the transaction processing server automatically, normally making use of a fixed line telecommunication network.

In the normal course of events, using current authorisation systems, the transaction is authorised or declined in a process of communication between the transaction processing server and the financial services provider. The result of this authorisation process is then communicated back to the transaction processing client by way of the fixed line network.

It will be appreciated that the network need not be a fixed line network, particularly since mobile communication networks are being used with increasing frequency in situations such as this.

A number of credit card fraud schemes in current use are unlikely to be detected in a simple authorisation process such as this, particularly where a credit card is duplicated or cloned.

For this reason the system of the invention proposes the use, essentially, of a two-part authorisation process – one that includes a first, transaction initiation component and a final transaction authorisation component, the latter directed at final transaction authorisation by the transaction initiator.

Using the simple credit card transaction described above, the example of the invention illustrated in the flow chart directs the transaction initiation component on a conventional communications stream, using the POS terminal (the transaction processing client) and the transaction processing server and financial services provider in their normal functions. At this point, however, the process loops into a final transaction authorisation component that requires final authorisation by the transaction initiator – the card holder who has authority over the account – using a separate communications stream constituted by a mobile communications network.

In the example illustrated, the communications network is a GSM network on which data

transfer is undertaken by way of SMS communications. It will be appreciated that GPRS (General Packet Radio Service) communication protocols would work equally well, if not better.

Referring to the flow chart, the card holder as transaction initiator, initiates a transaction at the POS terminal that serves as a transaction processing client. Transaction data is entered into the transaction processing client, which data is normally constituted by the transaction value and details of the transaction initiators credit card account, which details are obtained in conventional fashion by swiping the credit card through a magnetic stripe reader forming part of the transaction processing client.

The transaction processing client then, as in the conventional process, dials out to the transaction processing server forming part of the financial services provider network and transmits the transaction data together with the transaction initiator account data to the transaction processing server as a transaction authorisation request.

The financial records of the financial services provider are available to the transaction processing server and on receipt by the transaction processing server, these records are interrogated by the transaction processing server to determine whether or not the transaction is financially permissible – essentially to determine whether or not the transaction initiator's credit card account has sufficient credit to permit the transaction. If not, the transaction processing server simply transmits a signal to the transaction processing client to the effect that the transaction is not authorised, as occurs normally in present day transaction processing systems.

If the transaction is financially permissible, the transaction processing server looks up the appropriate communications data of the card holder or transaction initiator in the databases of the financial services provider, in this case the mobile phone number of the transaction initiator. The transaction processing server then transmits a transaction authorisation request to a telecommunications server which, in this, example, will be constituted by an SMS gateway. On receipt, the telecommunications server converts the transaction authorisation request to an SMS, which it sends to the telecommunications client constituted by the card holder's mobile phone.

It will be appreciated that the SMS gateway must, of necessity, be one that enjoys priority

routing on the mobile communications network so as not to introduce inordinate delays in the transaction authorisation process.

The card holder now receives an SMS on his or her mobile phone requesting authorisation of the transaction. If the card holder is not the transaction initiator, then the card holder can cancel the transaction immediately, and, if necessary, alert the financial services provider and possibly the police that fraud is being perpetrated.

Upon accepting the option of not authorising (or canceling) the transaction, normally by pressing the appropriate key on the mobile phone, the card holder sends an SMS to the telecommunications server which converts the SMS and sends a cancellation signal to the transaction processing client via the transaction processing server. The POS terminal, as transaction processing client, will then display a message to the effect that the transaction cannot be authorised.

In the normal course of events the card holder will be the transaction initiator.

The mobile phone, as telecommunications client, is programmed to display the SMS containing the transaction authorisation request and to await the entry of an authorisation code. This code will normally take the form of a personal identification number (PIN) previously supplied to the card holder by the financial services provider or selected by the card holder, as the case may be.

Should the card holder elect to accept the option of authorising the transaction, then by pressing the appropriate key, the mobile phone sends an SMS to the telecommunications server.

The SMS from the mobile phone (serving as telecommunications client) may contain PIN and transaction data that is sent via the telecommunications server, to the transaction processing server.

On receipt by the transaction processing server, the transaction and PIN data is verified. In particular, the PIN data is verified against card holder account data held by the financial services provider. If, for some reason, the PIN data is found to be invalid, a cancellation signal is sent to the transaction processing client which displays a message to the effect that

the transaction cannot be authorised.

In the normal course and since the PIN data has already gone through a verification step in the telecommunications client, the PIN data will be valid, in which case the transaction data will be transmitted to the financial services provider for processing, normally by debiting the account of the card holder.

The transaction processing server also transmits a transaction authorisation signal to the point of sale terminal as transaction processing client, which displays a message to the effect that the transaction has been authorised and produces the normal credit card slips for signature by the card holder and transaction initiator.

Whilst the system has been described above with reference to a credit card transaction, the system will work equally well in the verification of the authorisation of other financial transactions.

For instance, if the transaction processing client is a computer serving as an internet terminal, the procedure will be almost identical, once again requiring the card holder or account holder, as transaction initiator, to enter a PIN number on his or her mobile phone to verify the authorisation of the transaction.

Once again, the transaction initiation component and transaction authorisation component of the process are carried out on separate communication streams, with the final authorisation being provided by the mobile phone of the transaction initiator.

With the appropriate point of sale terminal, either in the form of a keypad, a cheque reader or both, the system of the invention can also be adapted to the verification of cheque-based transactions.

The transaction verification process follows the course outlined above, with the personal authorisation of the transaction initiator being required by way of a PIN code entered on a relatively personal device – the mobile phone of the transaction initiator - to provide final verification of the transaction.

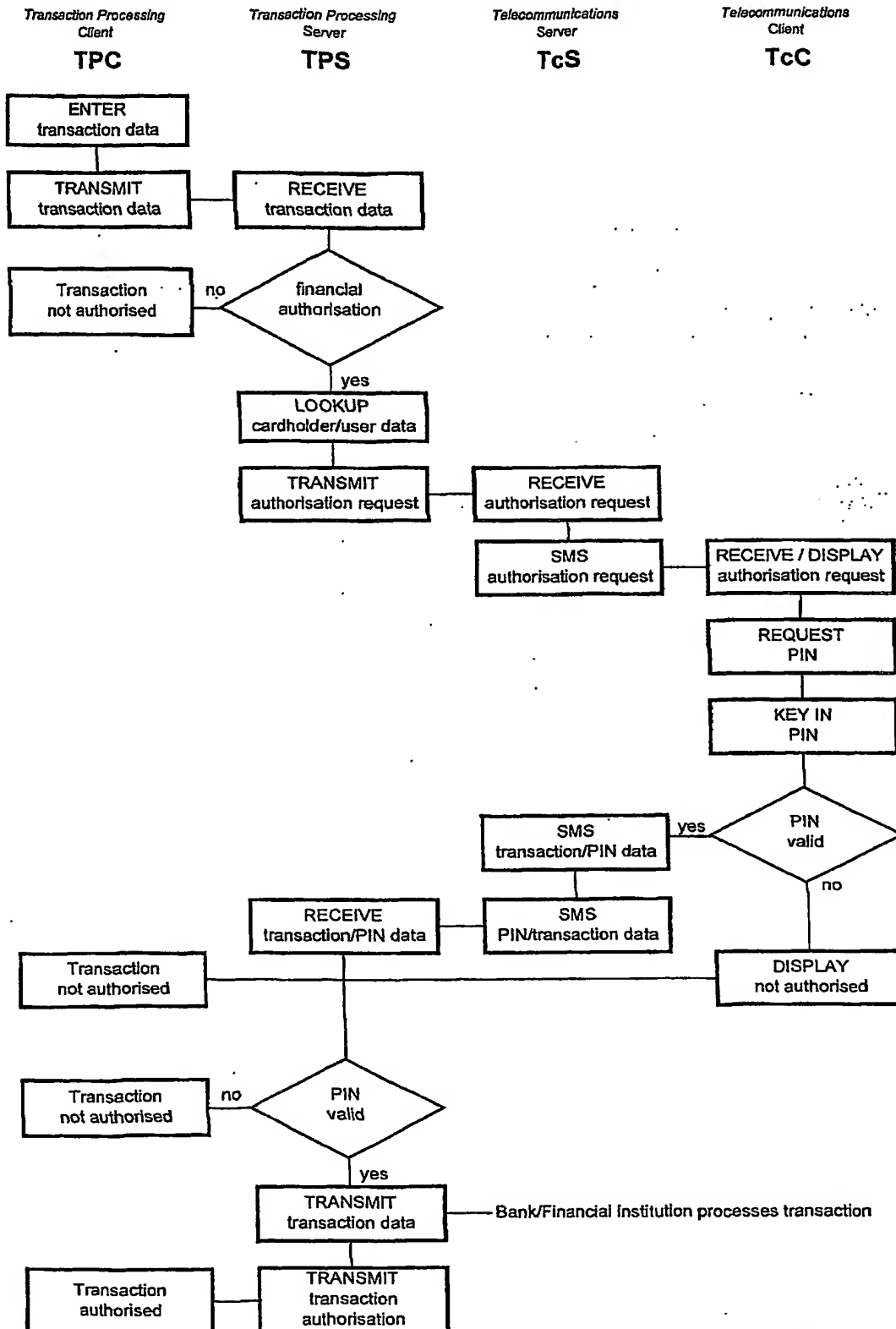
Various forms of data encryption may be used to encrypt the messages and signals

transmitted as part of this transaction authorisation and verification process, particularly bank account and PIN code data.

The financial transaction process related above is but one example of the transaction processing capacity of the system.

Dated 4 November 2003

  
 .....  
**PFT Burger Patent & Trade Mark Attorneys**  
 Applicant's Patent Attorneys



# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/ZA04/000072

International filing date: 30 June 2004 (30.06.2004)

Document type: Certified copy of priority document

Document details: Country/Office: ZA  
Number: 03/8654  
Filing date: 06 November 2003 (06.11.2003)

Date of receipt at the International Bureau: 28 January 2005 (28.01.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland  
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse